

PATENT ABSTRACTS OF JAPAN

AE

(11)Publication number : 2004-328199

(43)Date of publication of application : 18.11.2004

(51)Int.Cl. H04Q 7/38
H04B 7/26
H04L 9/34

(21)Application number : 2003-118107

(71)Applicant : DENSO CORP

(22)Date of filing : 23.04.2003

(72)Inventor : SHIRAKI HIDENAO
MATSUGATANI KAZUOKI

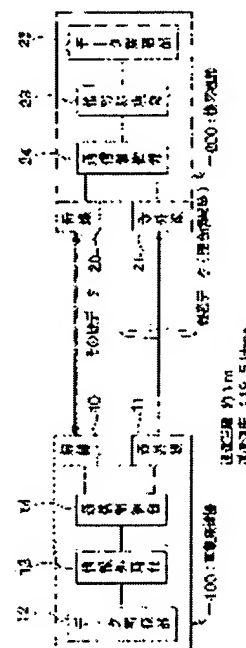
(54) PORTABLE DEVICE AND ON-VEHICLE RADIO EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To suppress wiretapping of secret data beforehand.

SOLUTION: A portable device 200 uses infrared rays as a medium to transmit secret data to on-vehicle radio equipment 100 and uses radio waves as a medium to transmit data other than secret data to the on-vehicle radio equipment 100. Since infrared communication has a shorter communication distance and a higher rectilinear propagation property than communication using radio waves as a medium, a wiretapper must come close to the on-vehicle radio equipment 100 to receive secret data when the secret data is transmitted by infrared communication.

Consequently, there is a high probability that the wiretapper is visually found by a driver or the like.



LEGAL STATUS

[Date of request for examination]

17.05.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-328199

(P2004-328199A)

(43) 公開日 平成16年11月18日(2004. 11. 18)

(51) Int. Cl.⁷

H04Q 7/38

H04B 7/26

H04L 9/34

F I

H04B 7/26 109R

H04L 9/00 681

H04B 7/26 109G

H04B 7/26 E

テーマコード(参考)

5J104

5K067

審査請求 未請求 請求項の数 8 O L (全 14 頁)

(21) 出願番号

特願2003-118107(P2003-118107)

(22) 出願日

平成15年4月23日(2003. 4. 23)

(71) 出願人 000004260

株式会社デンソー

愛知県刈谷市昭和町1丁目1番地

(74) 代理人 100100022

弁理士 伊藤 洋二

(74) 代理人 100108198

弁理士 三浦 高広

(74) 代理人 100111578

弁理士 水野 史博

(72) 発明者 白木 秀直

愛知県刈谷市昭和町1丁目1番地 株式会
社デンソー内

(72) 発明者 松ヶ谷 和沖

愛知県刈谷市昭和町1丁目1番地 株式会
社デンソー内

最終頁に続く

(54) 【発明の名称】 携帯機器および車載無線機

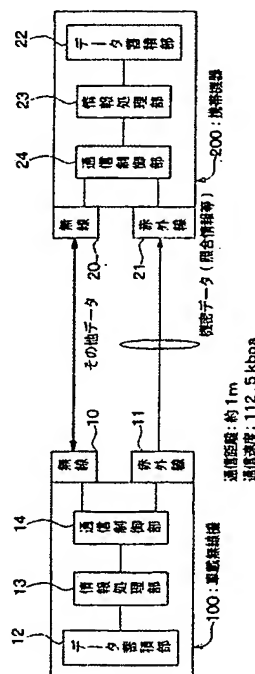
(57) 【要約】

【課題】 機密データが盗聴されることを未然に抑制する。

【解決手段】 携帯機器200では、赤外線を媒体として機密データを車載無線機100に送信し、機密データ以外のデータを電波を媒体として車載無線機100に送信している。ここで、赤外線通信は、電波を媒体とする用いる場合に比べて、その通信距離が短く、直進性が強い。そのため、機密データを赤外線通信により送信したときに、その送信された機密データを盗聴を受信しようとしても、その泥棒が、車載無線機100の近くに近寄った受信する必要がある。したがって、その泥棒が、乗員等に黙視で見つける可能性が高い。

【選択図】

図1



【特許請求の範囲】**【請求項1】**

車載無線機との間で無線通信を行うための携帯機器であって、赤外線を媒体として機密データを前記車載無線機に送信する第1の送信手段(21)と、前記機密データ以外のデータを電波を媒体として前記車載無線機に送信する第2の送信手段(20)と、を有することを特徴とする携帯機器。

【請求項2】

車載無線機との間で無線通信を行うための携帯機器であって、送信データを複数個に分割して複数個の分割データを生成する分割手段(S300)と、前記複数個の分割データのうち少なくとも1つの分割データ以外の他の分割データを電波を媒体として前記車載無線機に送信する第1の送信手段(S305)と、前記少なくとも1つの分割データを赤外線を媒体として前記車載無線機に送信する第2の送信手段(S304)と、を有することを特徴とする携帯機器。

10

【請求項3】

前記1つの分割データと、前記他の分割データとを用いて演算する演算手段(S302)を有し、前記第1の送信手段は、前記他の分割データとして前記演算手段の演算結果を前記車載無線機に送信するものであることを特徴とする請求項2に記載の携帯機器。

【請求項4】

車載無線機との間で無線通信を行うための携帯機器であって、送信データを複数個に分割して複数個の分割データを生成する分割手段と、前記複数個の分割データのうち少なくとも1つの分割データを用いて、この1つの分割データ以外の他の複数の分割データを並べる順番を決める決定手段と、前記他の複数の分割データを前記決定手段により決定された順番で並べるとともに、この並べられた他の複数の分割データを電波を媒体として前記車載無線機に送信する第1の送信手段と、前記少なくとも1つの分割データを赤外線を媒体として前記車載無線機に送信する第2の送信手段と、を有することを特徴とする携帯機器。

20

【請求項5】

携帯機器との間で無線通信を行うための車載無線機であって、電波を媒体として機密データを前記携帯機器に送信する第1の送信手段と、前記機密データ以外のデータを赤外線を媒体として前記携帯機器に送信する第2の送信手段と、を有することを特徴とする車載無線機。

30

【請求項6】

携帯機器との間で無線通信を行うための車載無線機であって、送信データを複数個に分割して複数個の分割データを生成する分割手段と、前記複数個の分割データのうち少なくとも1つの分割データ以外の他の分割データを電波を媒体として前記携帯機器に送信する第1の送信手段と、前記少なくとも1つの分割データを赤外線を媒体として前記携帯機器に送信する第2の送信手段と、を有することを特徴とする車載無線機。

40

【請求項7】

前記1つの分割データと、前記他の分割データとを用いて演算する演算手段を有し、前記第1の送信手段は、前記他の分割データとして前記演算手段の演算結果を前記携帯機器に送信するものであることを特徴とする請求項6に記載の車載無線機。

【請求項8】

携帯機器との間で無線通信を行うための車載無線機であって、送信データを複数個に分割して複数個の分割データを生成する分割手段と、前記複数個の分割データのうち少なくとも1つの分割データを用いて、この1つの分割データ以外の他の複数の分割データを並べる順番を決める決定手段と、前記他の複数の分割データを前記決定手段により決定された順番で並べるとともに、この

50

並べられた他の複数の分割データを電波を媒体として前記携帯機器に送信する第1の送信手段と、
前記少なくとも1つの分割データを赤外線を媒体として前記携帯機器に送信する第2の送信手段と、を有することを特徴とする車載無線機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、携帯機器およびこの携帯機器との間で無線通信を行う車載無線機に関する。

【0002】

【従来の技術】

近年、例えば、携帯電話等の携帯機器と車載無線機とで相互通信を行うのに、クレードルと呼ばれる接続装置を用いて携帯機器および車載無線機の間を有線で接続することが主流となっている。しかし、乗員が携帯機器を携帯して乗車する際には、クレードルに携帯機器をセットしたり、また、乗員が下車する際には、クレードルから携帯機器を取り外したりすることが必要であるため、手間がかかり、利便性に乏しかった。

【0003】

これに対して、携帯機器のセットや取り外しの手間を省くために、携帯機器及び車載無線機の間を電波を媒体として相互通信を行う車載無線システムが提案されている（例えば、特許文献1参照）。

【0004】

【特許文献1】

特開2001-218262号公報

【0005】

【発明が解決しようとする課題】

ところで、上述の車載無線システムでは、車載無線機の盗難を防止するために、携帯機器が車載無線機に接近したときに、車載無線機が携帯機器から送られる照合データを照合してアクティブ状態になるようにする。しかし、照合データは、携帯機器から電波を媒体として送信されるものであるため、この照合データが車室外に漏れて、車外で盗聴される可能性がある。

【0006】

本発明は、上記点に鑑み、送信データの盗聴を抑制するようにした携帯機器および車載無線機を提供することを目的とする。

【0007】

【課題を解決するための手段】

本発明は、上記目的を達成するために、請求項1に記載の発明では、車載無線機との間で無線通信を行うための携帯機器であって、赤外線を媒体として機密データを車載無線機に送信する第1の送信手段（21）と、機密データ以外のデータを電波を媒体として車載無線機に送信する第2の送信手段（20）と、を有することを特徴とする。

【0008】

ここで、赤外線は、電波よりも、直進性が強く、また、赤外線を用いた通信は、電波を用いた通信よりも、その通信可能距離が短い。したがって、機密データを赤外線を媒体として機密データを車載無線機に送信した場合、その機密データを泥棒が違法に受信しようとしても、その泥棒が、車載無線機、携帯機器の近くに近寄る必要がある。このため、車載無線機、携帯機器のユーザに泥棒が見つかる可能性が高くなり、そのことが一般に広まれば、送信データの盗聴を抑制することができる。

【0009】

請求項2に記載の発明では、車載無線機との間で無線通信を行うための携帯機器であって、送信データを複数個に分割して複数個の分割データを生成する分割手段（S300）と、複数個の分割データのうち少なくとも1つの分割データ以外の他の分割データを電波を媒体として車載無線機に送信する第1の送信手段（S305）と、少なくとも1つの分割

10

20

30

40

50

データを赤外線を媒体として車載無線機に送信する第2の送信手段（S304）と、を有することを特徴とする。

【0010】

ここで、泥棒が、送信データを違法に受信しようとしても、その送信データの内容を知るには、1つの分割データ及び他の分割データの全てを受信する必要がある。しかし、1つの分割データは赤外線を媒体として送信されるものであるため、上述の請求項1に記載の発明と同様、泥棒が、1つの分割データを受信するためには、車載無線機、携帯機器の近くに近寄る必要があり、その泥棒がユーザに見つかる可能性が高く、そのことが一般に広まれば、送信データの盗聴を抑制することができる。

【0011】

特に、請求項3に記載の発明のように、1つの分割データと、他の分割データとを用いて演算する演算手段（S302）を有し、第1の送信手段は、他の分割データとして演算手段の演算結果を車載無線機に送信すれば、仮に、泥棒に違法に演算手段の演算結果が受信されても、他の分割データを加工することなく送信する場合に比べて、送信データを復元し難くなる。そのことが一般に広まれば、送信データの盗聴をより一層、抑制することができる。

【0012】

請求項4に記載の発明では、車載無線機との間で無線通信を行うための携帯機器であって、送信データを複数個に分割して複数個の分割データを生成する分割手段と、複数個の分割データのうち少なくとも1つの分割データを用いて、この1つの分割データ以外の他の複数の分割データを並べる順番を決める決定手段と、他の複数の分割データを決定手段により決定された順番で並べるとともに、この並べられた他の複数の分割データを電波を媒体として車載無線機に送信する第1の送信手段と、少なくとも1つの分割データを赤外線を媒体として車載無線機に送信する第2の送信手段と、を有することを特徴とする。

【0013】

これにより、1つの分割データは、赤外線を媒体として送信されるものであるため、泥棒が、1つの分割データを違法に受信しようとしても、その泥棒が、車載無線機、携帯機器の近くに近寄る必要がある。このため、請求項1～4に記載の発明と同様、車載無線機、携帯機器のユーザに泥棒が見つかる可能性が高くなる。

【0014】

また、泥棒が、仮に、他の複数の分割データを違法に受信しても、送信データを復元するには、他の複数の分割データを並び替える必要がある。したがって、泥棒としては、決定手段により決められた順番を知る必要があり、送信データを復元するのは困難となる。そのことが一般に広まれば、送信データの盗聴を抑制することができる。

【0015】

また、上述の請求項1～4に記載の発明を、携帯機器ではなく、車載無線機に適用してもよい。

【0016】

具体的には、請求項5に記載の発明のように、携帯機器との間で無線通信を行うための車載無線機であって、電波を媒体として機密データを携帯機器に送信する第1の送信手段と、機密データ以外のデータを赤外線を媒体として携帯機器に送信する第2の送信手段と、を有するように構成してもよい。

【0017】

また、請求項6に記載の発明のように、携帯機器との間で無線通信を行うための車載無線機であって、送信データを複数個に分割して複数個の分割データを生成する分割手段と、複数個の分割データのうち少なくとも1つの分割データ以外の他の分割データを電波を媒体として携帯機器に送信する第1の送信手段と、少なくとも1つの分割データを赤外線を媒体として携帯機器に送信する第2の送信手段と、を有するように構成してもよい。

【0018】

請求項7に記載の発明では、1つの分割データと、他の分割データとを用いて演算する演

10

20

30

40

50

算手段を有し、第1の送信手段は、他の分割データとして演算手段の演算結果を携帯機器に送信するように構成してもよい。

【0019】

請求項8に記載の発明では、携帯機器との間で無線通信を行うための車載無線機であって、送信データを複数個に分割して複数個の分割データを生成する分割手段と、複数個の分割データのうち少なくとも1つの分割データを用いて、この1つの分割データ以外の他の複数の分割データを並べる順番を決める決定手段と、他の複数の分割データを決定手段により決定された順番で並べるとともに、この並べられた他の複数の分割データを電波を媒体として携帯機器に送信する第1の送信手段と、少なくとも1つの分割データを赤外線を媒体として携帯機器に送信する第2の送信手段と、を有するように構成してもよい。

10

【0020】

因みに、上記各手段の括弧内の符号は、後述する実施形態に記載の具体的手段との対応関係を示す一例である。

【0021】

【発明の実施の形態】

(第1実施形態)

図1に本発明の第1実施形態の車載無線システムを示す。車載無線システムは、車載無線機100及び携帯機器200から構成されている。車載無線機100は、第1の無線部10、第2の無線部11、データ蓄積部12、情報処理部13、および通信制御部14から構成されている。

20

【0022】

第1の無線部10は、アンテナ及び無線回路から構成されて、携帯機器200から電波を媒体として送信される信号を受信するとともに、送信信号を電波を媒体として送信する。

【0023】

第2の無線部11は、赤外線を出射する発光ダイオード、および赤外線を受光して出力信号を出力する受光ダイオードから構成されて、携帯機器200から赤外線を媒体として送信される信号を受信するとともに、送信信号を赤外線を媒体として送信する。

【0024】

なお、第2の無線部11の通信速度としては、例えば、112.5Kbpsが用いられ、また通信距離としては約1mが用いられる。

30

【0025】

データ蓄積部12は、DRAM、SRAM、不揮発性メモリなどから構成されて、照合データ(パスワード)、個人情報情報(名前、住所、電話番号、クレジットカード情報)、リンク確立を確認するための問い合わせ情報(ポーリング情報)など機密性の高いデータを記憶する。

【0026】

また、情報処理部13は、各種のデータに対してフラグの追加などの信号処理を実行する。通信制御部14は、マイクロコンピュータや揮発性メモリなどから構成されて、データの種別に基づき第1、第2の無線部10、11のいずれを用いるかを決定するための処理を実行する。

40

【0027】

また、携帯機器200は、第1の無線部20、第2の無線部21、データ蓄積部22、情報処理部23、および通信制御部24から構成されている。第1の無線部20は、アンテナ及び無線回路から構成されて、車載無線機100から電波を媒体として送信される信号を受信する。第2の無線部21は、赤外線を出射する発光ダイオード、および赤外線を受光して出力信号を出力する受光ダイオードから構成されて、車載無線機100から赤外線を媒体として送信される信号を受信する。

【0028】

データ蓄積部22は、不揮発性メモリなどから構成されて、照合データ(パスワード)、個人情報情報(名前、住所、電話番号、クレジットカード情報)、リンク確立を確認する

50

ための問い合わせ情報（ポーリング情報）など機密性の高いデータを記憶する。

【0029】

情報処理部23は、各種のデータに対してフラグの追加などの信号処理を施す。通信制御部24は、マイクロコンピュータや揮発性メモリなどから構成されて、データの種別に基づき第1、第2の無線部20、21のいずれを用いるかを決定するための処理を実行する。

【0030】

次に、本実施形態の車載無線機100の通信制御部14及び携帯機器200の通信制御部24の作動について図2～図6を用いて説明する。図2は携帯機器200の通信制御部24の処理を示すフローチャート、図3(a)は図2の機器間照合処理の詳細を示すフローチャート、図3(b)は車載無線機100の通信制御部14の機器間照合処理の詳細を示すフローチャート、図4は、図2のデータ識別処理の詳細を示すフローチャート、図5は、図2のデータ送受信処理の詳細を示すフローチャートである。先ず、車載無線機100では、通信制御部14が第1の無線部11により呼出データを一定期間毎に送信させている。

【0031】

ここで、ユーザが携帯機器200を携帯して乗車すると、携帯機器200の通信制御部24が、第1の無線部20により呼出データを受信する。これに伴い、呼出データの受信レベルが所定値以上の場合には、通信制御部24が、携帯機器200自体が車載無線機100に接近していると判定して、データ蓄積部22から、携帯機器200自身の識別を示す第1の照合データと呼び出してこの照合データを第2の無線部21から送信させる(S102)。

【0032】

その後、車載無線機100では、通信制御部14が第2の無線部21により第1の照合データを受信して、この受信される第1の照合データとデータ蓄積部12に予め記憶される第1の照合データとを照合して、互いに一致することを判定すると(S130: YES)、車載無線機100の通信制御部14がアクティブ状態になる。さらに、通信制御部14がデータ蓄積部12から、車載無線機100自身の識別を示す第2の照合データと呼び出してこの第2の照合データを第2の無線部11から送信させる(S131)。

【0033】

これに伴い、携帯機器200の通信制御部24が、第2の無線部20により第2の照合データを受信し、この受信される第2の照合データと、データ蓄積部22に予め記憶される第2の照合データとを照合し、互いに一致することを判定すると、データ識別処理(S110)に移行する。

【0034】

このデータ識別処理では、ユーザに対して、携帯機器200の図示しないキー操作部への操作により個人情報(すなわち、機密情報)を入力する際には、個人情報にフラグを付加させるものである。すなわち、個人情報をフラグとともにキー操作部への操作により入力されると(図4のS111)、通信制御部24が、情報処理部23により、個人情報(データ)、及びフラグ(これは、後述するように、個人情報が機密データであるか否かを識別するデータ)を合成させて(S112)、この合成されたフラグ付の個人情報を表示部(図示しない)によって表示させてユーザに対して再確認させる(S113)。

【0035】

その後、ユーザが、この表示されるフラグ付の個人情報を了承する旨を示す操作をキー操作部に対して行くと、フラグ付の個人情報をデータ蓄積部22に蓄積してデータ送受信処理(図2のS120)に移行する。このデータ送受信処理では、通信制御部24が、データ蓄積部22から順次データと呼出し、この呼び出されるデータ毎にこのデータが機密データ、すなわち、漏洩することを避けるべきデータであるか否かを判定する。

【0036】

ここで、データ蓄積部22から呼出したデータに、上述のフラグが付加されているもので

10

20

30

40

50

あるときには、この呼び出したデータには機密データ（例えば、個人情報）が含まれていると判定して、この呼び出されたデータ（機密データ＋フラグ）に、図6（b）に示すようにヘッダデータ（ヘッダ）を付加して第2の無線部21から赤外線を媒体として送信させる（S122、S124）。また、データ蓄積部22から呼び出されたデータが、機密データでないと判定したとき、この呼び出されたデータ（一般データ）に、図6（a）に示すようにヘッダデータ（ヘッダ）を付加して第1の無線部21から電波を媒体として送信させる（S123、S124）。

【0037】

その後、車載無線機100の通信制御部14では、第1の無線部10により電波を媒体としてデータを受信すると、この受信データをデータ蓄積部22に蓄積する。一方、通信制御部14が、第2の無線部11により赤外線を媒体としてデータを受信すると、この受信データをフラグと機密データとに分解して、この分解された機密データをデータ蓄積部22に蓄積する。

【0038】

以下、本実施形態の作用効果につき述べる。携帯機器200では、赤外線を媒体として機密データを車載無線機100に送信し、機密データ以外のデータを電波を媒体として車載無線機100に送信している。ここで、赤外線を媒体として用いる通信（以下、赤外線通信という）は、電波を媒体とする用いる場合に比べて、その通信距離が短く、直進性が強い。

【0039】

そのため、本実施形態のように、機密データを赤外線通信により車載無線機100に送信したときに、その送信された機密データを盗聴、すなわち、違法に機密データを受信しようとしても、その泥棒が、車載無線機100の近くに近寄った受信する必要がある。したがって、その泥棒が、乗員等に黙視で見つかる可能性が高く、そのことが一般に広まれば、機密データが盗聴されることを未然に抑制され得る。

【0040】

上述の本実施形態では、データ識別処理として、図4に示すように、例えば、個人情報などの機密情報はキー操作等で手入力されるもので、手入力でデータにフラグを付加して入力させるとその入力データをデータ蓄積部22に記憶させ、データにフラグが付加されているか否かによって、そのデータが機密情報であるか否かを判定する例を示したが、これに限らず、図7、図8に示すようにしてもよい。

【0041】

（1）例えば、外部からキー操作により入力されたとき、その入力データを誤って消去することを防止するために、入力データに対して読み取りだけのアクセスを許可するように設定されている場合には（図7のS111a）、この入力データは、機密情報であると判定して、その入力データにフラグを付加して表示部（図示しない）により表示させてユーザに再確認させてから（S112、S113）、その後データ蓄積部22に記憶させる。

【0042】

（2）例えば、外部からキー操作により入力されたとき、その入力データが機密データの場合には、データ蓄積部22のうち特定のフォルダ（以下、フラグフォルダという）に記憶させる。そして、定期的にフラグフォルダからそのフラグフォルダに含まれるデータを呼出しその呼び出されるデータにフラグを付加して表示部（図示しない）により表示させてユーザに再確認させてから（図8のS111a～S113）、その後、データ蓄積部22のうちフラグフォルダ以外のエリアに記憶させる。

【0043】

（第2実施形態）

上述の実施形態においては、携帯機器200が、データ送信を行う際には、データの種別に応じて電波および赤外線のうちいずれを用いるかを決定する例について説明したが、これに代えて、本実施形態では、図9に示すように、携帯機器200が、データの種別に依存せず、赤外線および電波の双方を利用して送信データを送信するようにする。この場合

10

20

30

40

50

の携帯機器 200 の通信制御部 24 のデータ送受信処理を、図 11 に示す。以下、通信制御部 24 によるデータ送受信処理について図 11 を用いて説明する。

【0044】

先ず、通信制御部 24 は、図 11 に示すフローチャートに従って、コンピュータプログラムを実行する。先ず、情報処理部 23 によりデータ蓄積部 23 から図 10 に示す送信データを呼出しこの呼出される送信データのうちヘッダを除くデータを N (N は自然数) 個に分割して、 N 個の分割データ $A_1 \sim A_N$ を生成させる (S300)。

【0045】

ここで、 N 個の分割データ $A_1 \sim A_N$ のうち先頭の分割データ A_1 を主キーとして、この主キーと分割データ $A_2 \sim A_N$ の個々として XOR 演算を行って演算データ $B_2 \sim B_N$ を求める (S301、S302)。

10

【0046】

例えば、演算データ B_2 は、図 12 に示すように、分割データ A_1 と分割データ A_2 とにより XOR 演算されたものであり $\{B_2 = A_1 (XOR) A_2\}$ 、演算データ B_3 は、分割データ A_1 と分割データ A_3 とにより XOR 演算されたものであり $\{B_3 = A_1 (XOR) A_3\}$ 、演算データ B_N は、分割データ A_1 と分割データ A_N とにより XOR 演算されたものである $\{B_N = A_1 (XOR) A_N\}$ 。

【0047】

以上のように演算データ $B_2 \sim B_N$ 及び分割データ A_1 が生成されると、分割データ A_1 を第 2 の無線部 21 により赤外線を媒体として送信させる。これに加えて、ヘッダを第 1 の無線部 20 により電波を媒体として送信させるとともに、演算データ $B_2 \sim B_N$ を、順次、第 1 の無線部 20 により電波を媒体として送信させる。

20

【0048】

その後、車載無線機 100 では、第 2 の無線部 11 で分割データ A_1 を受信し、ヘッダを第 1 の無線部 10 で受信するとともに、演算データ $B_2 \sim B_N$ を、順次、第 1 の無線部 10 で受信する。ここで、分割データ A_1 をキー種として、このキー種と演算データ $B_2 \sim B_N$ との個々として XOR 演算を行って分割データ $A_2 \sim A_N$ の個々を求める (S400、S401)。これに加えて、ヘッダ、分割データ A_1 、および分割データ $A_2 \sim A_N$ を合成して送信データを復元させる (S402)。

【0049】

30

以下、本第 2 実施形態の特徴につき述べる。すなわち、携帯機器 200 では、送信データを分解して分割データ $A_1 \sim A_N$ を生成して、分割データ $A_2 \sim A_N$ を電波を媒体として車載無線機に送信し、分割データ A_1 を赤外線を媒体として車載無線機に送信する。

【0050】

ここで、泥棒が、送信データを違法に受信しようとしても、分割データ $A_1 \sim A_N$ の全てを受信する必要がある。しかし、分割データ A_1 は赤外線を媒体として送信されるものであるため、上述の実施形態と同様、泥棒が、分割データ A_1 を受信するためには、車載無線機 100、携帯機器 200 の近くに近寄る必要があり、その泥棒がユーザに見つかる可能性が高く、そのことが一般に広まれば、送信データの盗聴を抑制することができる。

【0051】

40

ここで、本実施形態では、分割データ A_1 と、分割データ $A_2 \sim A_N$ とを用いて XOR 演算して演算データ $B_2 \sim B_N$ を求め、分割データ $A_2 \sim A_N$ として、演算データ $B_2 \sim B_N$ (演算手段の演算結果) を車載無線機 100 に送信しているので、仮に、泥棒により違法に演算データ $B_2 \sim B_N$ が受信されても、分割データ $A_2 \sim A_N$ を加工することなく送信する場合に比べて、送信データを復元し難くなる。そのことが一般に広まれば、送信データの盗聴をより一層、抑制することができる。

【0052】

また、本実施形態では、演算データ $B_2 \sim B_N$ を求めるのに、一般の暗号処理ではなく、XOR 演算を用いたので、信号処理を行う上で、負荷を軽減することができる。

【0053】

50

次に、送信データを分割する分割数：Nの最適値について図14、図15を用いて述べる。

【0054】

図14、図15において、縦軸は送信データの転送時間、横軸は分割数：Nを盗聴される危険度を示す。図14は、第1の無線部20による通信（電波を媒体とする通信）と第2の無線部21による通信（赤外線を媒体とする通信）とを同時に行う一例を示し、図15は、第1の無線部20による通信と第2の無線部21による通信とを時分割に行う一例を示す。

【0055】

図14、図15から分かるように、分割数：Nを増やすほど、送信データを転送中に盗聴される危険度、すなわち、送信データが盗聴される可能性が高くなる。 10

【0056】

そこで、第1の無線部20による通信と第2の無線部21による通信とを同時に行う場合には、図14において、転送時間が最大値となる場合の分割数 N_{max} 、及び、転送時間が最小値となる場合の分割数 N_{min} を求め、分割数 N_{max} 、及び、分割数 N_{min} の平均値 $\{(N_{max} + N_{min}) / 2\}$ を最適値として求める。

【0057】

また、第1の無線部20による通信と第2の無線部21による通信とを時分割で行う場合には、図15において、図14の場合と同様、分割数 N_{max} 、及び、分割数 N_{min} の平均値 $\{(N_{max} + N_{min}) / 2\}$ を最適値として求める。 20

【0058】

（第3の実施形態）

上述の第2実施形態では、先頭の分割データA1を主キーとして、この主キーと分割データA2～ANの個々でXOR演算を行って演算データB2～BNを求める例を示したが、これに代えて、図16に示すように、演算データB1～BNを求めるようにしてもよい。

【0059】

すなわち、分割データA1、A2でXOR演算を行って演算データB2（=A1（XOR）A2）を求め、この演算データB2と分割データA3とでXOR演算を行って演算データB3（=B2（XOR）A3）を求め、この演算データB3と分割データA4とでXOR演算を行って演算データB4（=B3（XOR）A4）を求め、その後、同様に、演算データB5…BNを求めるようにする。 30

【0060】

（その他の実施形態）

上述の実施形態では、分割データA1と分割データA2～ANの個々でXOR演算を行って演算データB2～BNを求め、演算データB2～BNを第1の無線部20から送信させて、分割データA1を第2の無線部21から送信させる例を示したが、これに代えて、演算データA2～ANを送信する順番を分割データA1を基に決めて、この決めた順番で演算データA2～ANを並び替えて第1の無線部20から送信させるようにしてもよい。

【0061】

具体的には、携帯機器200は、送信データをN個に分割して分割データA1～ANを生成する分割手段と、分割データA1～ANのうち少なくとも1つの分割データA1を用いて、この1つの分割データA1以外の他の複数の分割データA2～ANを並べる順番を決める決定手段と、他の複数の分割データA2～ANを決定手段により決定された順番で並べるとともに、この並べられた他の複数の分割データA2～ANを第1に無線部20から電波を媒体として車載無線機100に送信する第1の送信手段と、少なくとも1つの分割データA1を赤外線を媒体として第2の無線部21から車載無線機100に送信する第2の送信手段と、を有するように構成する。 40

【0062】

この場合、分割データA1は、赤外線を媒体として送信されるものであるため、泥棒が、 50

分割データA1を違法に受信しようとしても、その泥棒が、車載無線機100、携帯機器200の近くに近寄る必要がある。このため、上述の実施形態と同様、車載無線機100、携帯機器200のユーザに泥棒が見つかる可能性が高くなる。

【0063】

また、泥棒が、仮に、他の分割データA2～ANを違法に受信しても、送信データを復元するには、分割データA2～ANを並び替える必要がある。したがって、泥棒としては、分割データA2～ANを送信する順番を知る必要があり、送信データを復元するのは困難となる。そのことが一般に広まれば、送信データの盗聴を抑制することができる。

【0064】

以上のように分割データA2～ANを並び替えて送信するのを携帯機器100ではなく、車載無線機200に適用してもよい。

10

【0065】

上述の第1、第2実施形態では、携帯機器100から車載無線機200にデータを送信する例を示したが、これに代えて、車載無線機200から携帯機器100に送信するようにしてもよい。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る車載無線システムの構成を示す図である。

【図2】図1の携帯機器の通信制御部の処理の概略を示すフローチャートである。

【図3】図2の処理の一部の詳細を示すフローチャートである。

【図4】図2の処理の一部の詳細を示すフローチャートである。

20

【図5】図2の処理の一部の詳細を示すフローチャートである。

【図6】データの送信フォーマットを示す図である。

【図7】第1の実施形態の変形例を示すフローチャートである。

【図8】第1の実施形態の変形例を示すフローチャートである。

【図9】本発明の第2実施形態に係る車載無線システムの構成を示す図である。

【図10】図9の携帯機器の情報処理部による処理を説明する為の図である。

【図11】図9の携帯機器の通信制御部によるデータ送信処理を示すフローチャートである。

【図12】図10の携帯機器の通信制御部によるデータ送信処理を説明するための図である。

30

【図13】車載無線部の通信制御部によるデータ受信処理を示すフローチャートである。

【図14】第2実施形態において盗聴の危険度を説明するための図である。

【図15】第2実施形態において盗聴の危険度を説明するための図である。

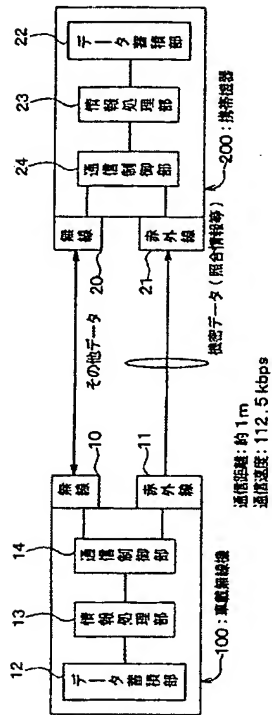
【図16】本発明の第3実施形態においてXOR演算を説明する為の図である。

【符号の説明】

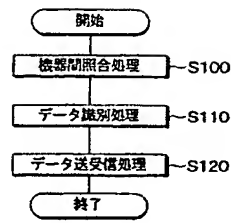
10、11、20、21…無線部、12、22…データ蓄積部、
13、23…情報処理部、24、14…通信制御部、
100…車載無線機、200…携帯機器。

40

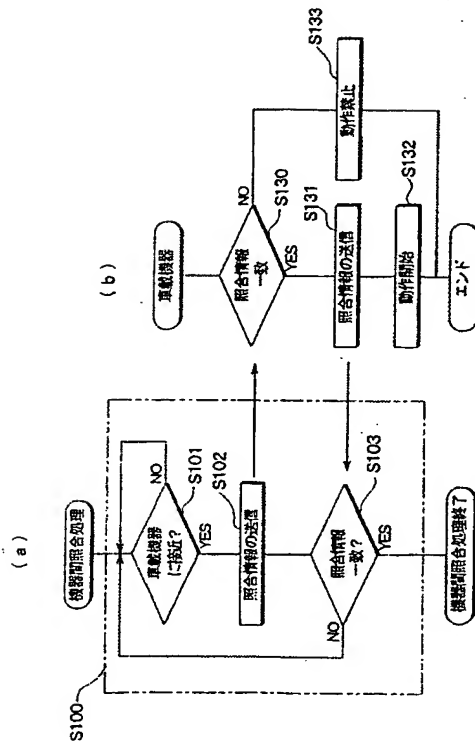
【図1】



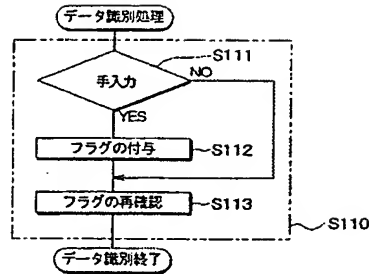
【図2】



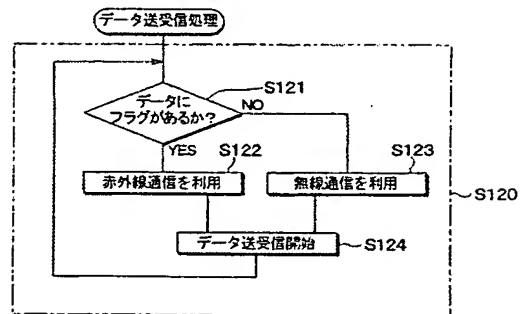
【図3】



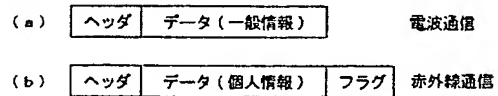
【図4】



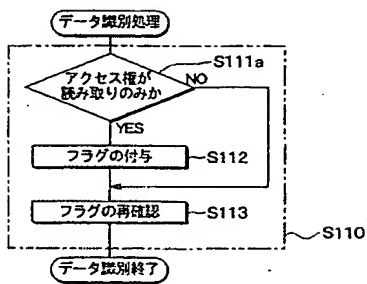
【図5】



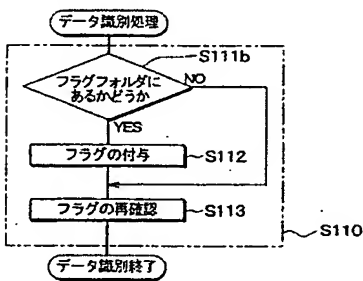
【図6】



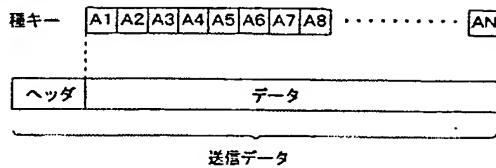
【図7】



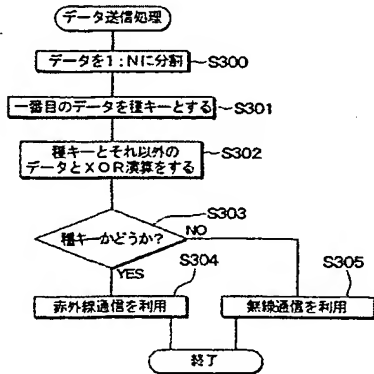
【図8】



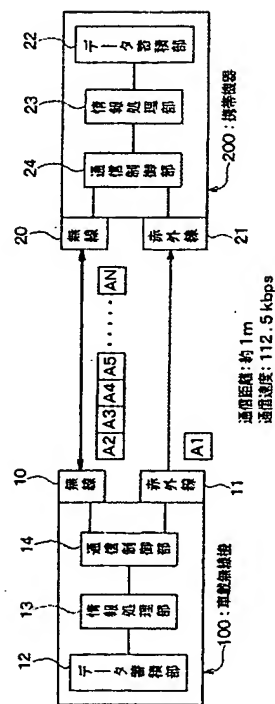
【図10】



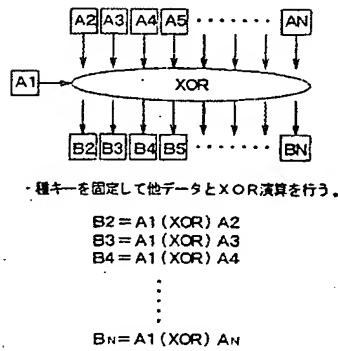
【図11】



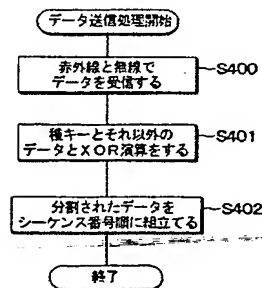
【図9】



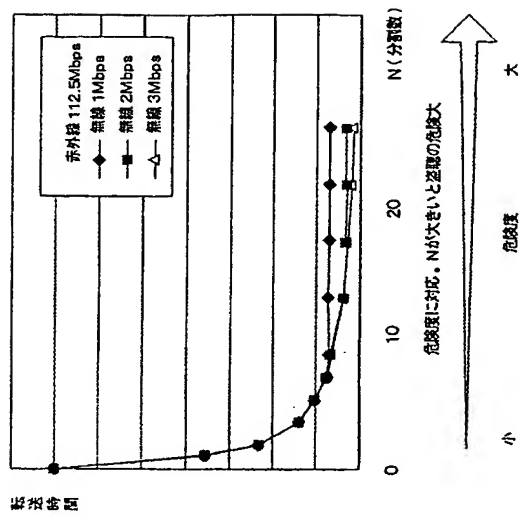
【図12】



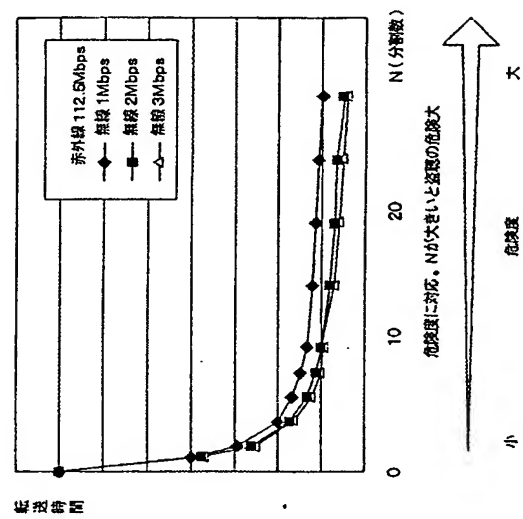
【図13】



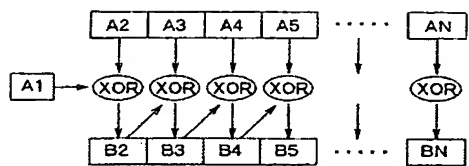
【図14】



【図15】



【図16】



前のデータを種キーとして順番にXOR演算を行う。

$$B2 = A1(XOR)A2$$

$$B3 = B2(XOR)A3$$

$$B4 = B3(XOR)A4$$

...

$$BN = B_{N-1}(XOR)AN$$

フロントページの続き

Fターム(参考) 5J104 AA01 AA02 AA03 AA16 EA18 EA21 JA03 NA02 NA09 NA24

PA02

5K067 AA30 BB03 BB04 EE04 EE32 EE37 FF07 GG06 HH22 HH24